Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	98	("6332077" "6345043" "5898679" "5991287" "6115411" "5509027" "5513210" "5583866" "5621798" "5594731" "5654959" "6539237" "6807431" "5515509" "5812531" "5901362" "5917865" "6360264" "6505045" "6577609" "6636737" "6711148" "6771933" "6873611" "6272129" "6772331" "6148405" "6651105" "5745884" "5771353" "5994998" "6140911" "5539824" "6430395" "6687243" "6782260" "6021495" "6766453" "5909462" "6549786" "6680924" "6151628" "6075860" "6084969" "6834341" "5768531" "6115390" "6327254" "5384777" "6070184").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2005/04/21 11:15
L2	66	l1 and ("wireless" with ("local area network" or "LAN"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2005/04/21 11:16
L3	67	l1 and ("wireless" with ("local area network" or "LAN" or "WLAN" or ("wireless" adj "LAN")))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2005/04/21 11:16
L4	47	l3 and (("access point" or transceiv$3 or (receiv$3 and (transmit$3 or send$3))) with ("intranet" or "local" or "without firewall" or "WLAN" or "LAN" ("local" adj "area" adj "network")))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2005/04/21 11:19
L5	10	l4 and (("access point" or transceiv$3 or (receiv$3 and (transmit$3 or send$3))) with (authenticat$3 near$3 ("wireless" adj ("unit" or "device" or "system"))))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2005/04/21 11:18
L6	6	l5 and (("firewall" or "gateway" or "router" or "bridge") with (("local" adj "area" adj "network") or "LAN"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2005/04/21 11:18

```
File 275:Gale Group Computer DB(TM) 1983-2005/Apr 20
         (c) 2005 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Apr 20
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Apr 20
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Apr 19
         (c) 2005 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2005/Apr 20
         (c)2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Apr 19
         (c) 2005 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2005/Apr 19
         (c) 2005 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2005/Apr W1
         (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Apr W3
         (c) 2005 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2005/Apr 19
         (c) 2005 The Dialog Corp.
File 369:New Scientist 1994-2005/Mar W3
         (c) 2005 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2005/Apr 20
         (c) 2005 Business Wire.
File 613:PR Newswire 1999-2005/Apr 20
         (c) 2005 PR Newswire Association Inc

Set     Items   Description
S1     318048   ACCESS()POINT? ? OR AP OR APS OR BASE()STATION? ? OR WIREL-
             ESS()(ROUTER? ? OR GATEWAY? ?)
S2          93   S1(5W)(AUTHENTICATED OR VALIDATED OR VERIFIED)
S3           5   S1(5W)((AUTHENTICATE OR AUTHENTICATES OR AUTHENTICATING OR
              VALIDATE OR VALIDATES OR VALIDATING)(1W)(ITSELF OR OWN()SELF -
              OR THEMSELVES))
S4         171   (AUTHENTICAT??? OR VALIDAT??? OR VERIF?)(1W)S1
S5         265   S2:S4
S6         136   RD (unique items)
S7          38   S6 NOT PY=2000:2005
S8        2251   MUTUAL?()(AUTHENTICAT??? OR VALIDAT??? OR VERIF?)
S9          68   S1(10N)S8
S10         30   RD (unique items)
S11          2   S10 NOT (S7 OR PY=2000:2005)
```

```
File 275:Gale Group Computer DB(TM) 1983-2005/Apr 20
         (c) 2005 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Apr 20
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Apr 20
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Apr 19
         (c) 2005 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2005/Apr 20
         (c)2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Apr 19
         (c) 2005 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2005/Apr 20
         (c) 2005 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2005/Apr W1
         (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Apr W3
         (c) 2005 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2005/Apr 19
         (c) 2005 The Dialog Corp.
File 369:New Scientist 1994-2005/Mar W3
         (c) 2005 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2005/Apr 20
         (c) 2005 Business Wire.
File 613:PR Newswire 1999-2005/Apr 20
         (c) 2005 PR Newswire Association Inc

Set     Items   Description
S1     150810   ACCESS()POINT? ? OR BASE()STATION? ? OR WIRELESS()(ROUTER?
              ? OR GATEWAY? ?)
S2       1938   S1(5N)(ROGUE OR FAKE OR IMPOSTER OR COUNTERFEIT OR BOGUS OR
               PHONY OR INTRUDER OR UNAUTHORIZED OR UNAUTHORISED OR (UN OR -
              .NOT. OR T)()(AUTHORIZED OR AUTHORISED) OR SPOOFED OR INVALID
              OR FALSE)
S3          0   S1(5N)("NOT"()(AUTHORIZED OR AUTHORISED))
S4        820   S1(5N)AUTHENTICAT?
S5         72   S2(50N)S4
S6         38   RD (unique items)
S7          0   S6 NOT PY=2000:2005
```

01784999 Supplier Number: 53533767 (THIS IS THE FULLTEXT)

SSH Communications Security Delivers Standards-based Virtual Private Networking (VPN) Cryptographic Security to Xedia Corporation.

PR Newswire, p0630
Jan 8, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 476

TEXT:

SSH Communications Security's SSH ISAKMP/Oakley Enables Internet Key Exchange (IKE) Functionality in Xedia(R) Corporation's Access Point(TM) QVPN(TM) Products

ESPOO, Finland, Jan. 8 /PRNewswire/ -- Xedia's Access Point QVPN is the industry's first Internet access platform to integrate high performance IP routing, Class-Based Queuing bandwidth management, VPN security and traffic measurement services in a single platform designed to enable network providers to deliver secure, business-quality Internet services.

The SSH ISAKMP/Oakley (SSH IKE) is a key security feature of Xedia's Access Point QVPN products. SSH ISAKMP/Oakley provides Access Point QVPN with key components to enable the most secure, interoperable and complete IPSec solution in the market.

SSH ISAKMP/Oakley is a tailor made toolkit for adding automatic key management and authentication into IPSec based networking devices. It supports the Internet Key Exchange (IKE) which automatically **authenticates** the **Access Point** QVPN and clients connecting to it. It also negotiates the security policy and encryption keys in a secure manner. SSH ISAKMP/Oakley makes authentication secure, easy and hassle-free by supporting Public Key Infrastructure integration with X.509 digital certificates and by interoperating with the major Certificate Authority (CA) vendors.

IPSec (Internet Protocol Security) and IKE (Internet Key Exchange) are Internet Engineering Task Force (IETF) standards for protecting IP traffic using cryptography on the packet level. They are totally transparent to the user making an ideal way of creating a company's virtual private network. IPSec technology marks the transition from early tunneling to fully-fledged Internet VPN services.

About SSH Communications Security

SSH Communications Security Ltd. is an international software company specialized in demanding network security solutions. SSH provides cutting-edge, military strength cryptographic solutions for securing internet communications. The company's ssh (Secure Shell) application has become the de facto standard for secure logins, and is being used by hundreds of thousands of people in more than 50 countries. SSH IPSEC Express toolkit is the market leader in providing IPSEC (Internet Protocol Security) and IKE (Internet Key Exchange) technology to OEM customers. For more information, please see http://www.ipsec.com on the Internet.

About Xedia Corporation

Xedia Corporation, a privately-held, venture-backed corporation is leading the way with a new class of Internet access platform delivering the performance, security, and service level control network providers need to deliver the next generation of business class Internet services. Xedia's Access Point products have been Internet-certified by the industry leading Internet providers, including UUNET, PSINet and Sprint, and they are now being deployed in the most demanding business Internet services in the industry. The company is headquartered in Littleton, MA and can be reached at (978)952-6000. The Xedia Web site can be found at http://www.xedia.com.

Xedia is a registered trademark and Access Point and QVPN are trademarks of Xedia Corporation. All other brands and product names may be trademarks or registered trademarks of their respective owners.

7/9/22 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

10284330 SUPPLIER NUMBER: 20805059 (THIS IS THE FULL TEXT)
Air raid warnings. (fraud in the cellular telephone business)
Wittering, Stewart; Daniels, Guy; Warwick, Martyn
Communications International, v25, n5, p47(5)
May, 1998
ISSN: 0305-2109 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 3550 LINE COUNT: 00281

TEXT:

Cellular fraud costs the industry more than USS I billion a year worldwide. And at 50% per annum, it's growing three times faster than cellular operators' profits. In the second part of our special report on telecomms fraud, Stewart Wittering, Guy Daniels and Martyn Warwick cross their fingers and key in their PINs

Make no mistake, fraud is big, big, business. In pre-cellular days, operator's losses were comparatively small, but the 1990s mobile boom presented fraudsters with a golden opportunity to make some big bucks - and they took it.

Think on this, during 1993, one European cellular operator lost 40% of its call revenues to fraudsters. However, large though these losses were they pale into insignificance when set against today's figures - which are widely accepted as being well in excess of $1 billion a year.

An endless war of attrition

In 1992, UK losses due to handset clomng were put at about $1.5 million, (with a further $750,000 attributed to fraudulent applications). By 1995, it was estimated that one call in six was fraudulent and was costing the UK industry about $75 million a year.

One particular user personally ran up a bill for $23,000 worth of international calls within two days. Now that takes determination, dedication and a goodly supply of throat lozenges.

According to the Federation of Communications Services (FCS), during the current year the industry loss due to cloning, stolen airtime and stolen handsets will rise to $225 million. The cost to the consumer is not known, but they are the ones who pay in the end.

Massive financial and human resources have been devoted to combating and reducing cellular fraud. However, recent experience indicates that, no matter how sophisticated the new anti-fraud measures and technologies may become, swindlers will always find a way round them. Operators have to be constantly aware of the types of fraud being committed and must devise the best possible means of countering their effects. Failure to do so results in loss of public confidence in the industry in general and increases churn in individual service operations in particular.

The nature of the beast determines that detection rates and legislative sanctions will always lag behind changing fraud patterns, but governments are now fully awake to the seriousness of the situation and are doing something about it.

Tough on the causes of crime

In the UK, a new Telecommunications (Fraud) Act has come into force and gives the police real power: telephone cloners and those who fraudulently access airtime now face a prison sentence of up to five years.

That the police mean business was demonstrated at a recent trial in the UK city of Northampton. Two men were sentenced to two years in prison for providing new identities for a relatively small number of stolen phones. There is every probability, and every reason why, other European operators will follow the UK's tough line.

Perhaps the most difficult type of cellular fraud to detect is handset cloning. This involves the complete duplication of a legitimate terminal, including the mobile identification number (MIN), electronic serial number (ESN), and, in some cases, the subscriber's personal identification number (PIN). Cellular switches cannot readily distinguish between legitimate terminals and clones which successfully bypass pre-call validation checks.

Best of all, from the fraudster's perspective, the bill for the calls is passed on to the owner of the original handset.

Most clones continue to use the same MIN and ESN combination until denied service by the operator. Some sophisticated clones, however, use different combinations, producing 'tumbling' phones which avoid triggering alarms and early detection. Tumbling works by setting up the MIN and ESN to step-on in value each time a call is made. This creates the illusion that each successive call is made by a different caller.

The most common ways of obtaining MIN and ESN information is by theft of subscriber data from the offices of the operator, or by the use of a frequency scanner to intercept the data transmitted over the radio channel each time a call is made or received, or whenever the mobile terminal registers with the mobile switching centre (MSC).

Another way of obtaining the MIN and ESN is to set up a fake base station and antenna close to mobile terminals, which send their MIN-ESN combinations across the ether along with other, often highly confidential, information.

Sometimes the detection of cloning is made even more difficult by roaming fraud - when valid MIN and ESN combinations are stolen in one cellular area and used in another. In 1996 in the US, one call-sell operation exposed a mobile operator to more then $1 million worth of roaming charges in three days.

Furthermore, bills of as little as $100, if challenged and publicised, can lead to a loss of commercial confidence in an operator. That's why so many keep quiet about the extent to which they are defrauded and write-off the losses.

Cloned phones are also frequently used to run call-sell operations. In Europe, one sting involved the cloning of dozens of analogue phones, while taking out one GSM account in a false name. The cloned phones were then used to sell international call capacity. Although they were barred from making international calls, the cloned phones were used to call the GSM phone, which then rerouted the calls to overseas destinations.

Cloning is a huge global business. Many countries simply do not have the resources or legal tools effective enough to successfully combat cellular fraud. For example, in Venezuela cloning presently counts as a second degree crime punishable by a maximum penalty of five years in prison. However, the industry there is lobbying to have it made a first degree or premeditated crime, which carries a penalty of eight years. They reason that cloning should be put on a par with interference with fixed wireline communications - which is regarded as action against the security interests of the state.

In Europe and many other parts of the world, GSM has been a remarkable success. The technology is remarkably sophisticated and so far there have been no substantiated instances of cloned GSM terminals' in Europe.

The strength of GSM

Recently though, university researchers in the US said they had cracked GSM's A5 encryption algorithm. Well. It's always possible of course, but their assertion is hard to verify as they have so far rifled to substantiate the claim.

While we are in the Land of the Free, it is interesting to note that the US, the notion of what constitutes freedom is very limited where mobile communications is concerned.

PCS 1900, the US equivalent of GSM, actually uses a deliberately diluted form of encryption which permits government security agencies to monitor calls. What's more, encryption can even be turned off entirely in times of an undefined 'national emergency'.

The US law enforcement lobbies and their apologists say that this is to help in the fight against organised crime, but many civil libertarians are suspicious that there may be more fundamental issues of personal liberty and privacy at stake.

In Europe, confidence in GSM is rock solid - despite continued rumours that the French haven't even bothered to turn on their encryption system.

Real fake identities

Although handset cloning remains a problem, authentication regimes and radio-frequency fingerprinting have had some effect. As a result, criminals

have moved on to subscription identity fraud which is based on retail point of sale procedures and fake identities. Subscription fraud is at its worst (or best - depending which side of the fence you are on), in the US. In Los Angeles alone it is estimated that 8% of all cellular calls are fraudulent.

Subscription fraud involves the criminal assumption of the persona of an innocent potential subscriber and is based on the acquisition of genuine personal data such as social security or healthcare numbers. Armed with a real ID (but fronted with a photo of the miscreant) the fraudster applies to take out a cellular subscription. Checks show that the proposed subscriber is credit-worthy - and off they go.

Handsets are then cloned for onward sale to criminal gangs. The poor sap whose identity has been used eventually gets a bill for tens of thousands of dollars which, ultimately, the cellular operator usually has to bear. However, the innocent victim often ends up with the world's worst credit rating.

In an attempt to stem a rising fide, cellular industry players have banded together to form mutual protection alliances and to lobby trade bodies to co-ordinate anti-fraud measures.

One such group, the US-based Cellular Telecommunications Industry Association (CTIA), contacts the police whenever retail outlets report repeat attempts to obtain cellular service. It has resulted in hundred of prosecutions.

Another CTIA counter-measure is to send 'welcome' letters to new subscribers requesting confirmation that cellular service is required. When the subscriber calls, an identity check is run against a database. No match, no service. The system has cut the time that a fraudulent subscriber may be able to make calls from four weeks down to two.

The enemy within

But, even as subscription fraud begins to be addressed, the criminals are turning their attention elsewhere. Now bribery, blackmail and coercion are being used to force some cellular operator employees to reveal details of live numbers, new MIN and ESN combinations and to subvert security procedures.

The president of the CTIA, Tom McClure is uncompromising on this issue. "It is imperative that the industry takes a strong stand," he says. "Crooked employees are criminals. They should be arrested in public to serve as a deterrent to others. Those that do the crime should do the time."

Not that such pronouncements cut much ice with the criminals. For example, in the UK during 1996, some 12,000 mobile phones vanished every month - at an estimated loss of $75 million to both operators and users. By early this year, the number of units stolen per month had risen to 15,000.

Stolen instruments are simply rechipped and given a new identity. And, while theft and knowingly using a cloned phone is against the law in the UK, rechipping is perfectly legal.

To try and beat the practice, operators now provide customers with a unique and secure identification code which is burnt into the handset. The number can then be blacklisted by the operating network if anything goes wrong. However, while the theory seems fine, it has had little deterrent effect in practice.

A hard trail to follow

For example, once a new SIM card is inserted into a GSM handset, it can be used free from detection. And in the UK, handsets are sold at highly subsidised rates (the latest models, which cost some $900 each to produce, go to new subscribers for as little as $15 to $50).

In cases of highly organised theft, gangs of criminals have travelled across the UK taking out phoney subscriptions using false identifies. They then sell on the SIM cards, which covers the costs associated with their peripatetic lifestyles, and collect hundreds of handsets for export (the main purpose of their dubious trade) - which end up in places as far away as Hong Kong.

In Uruguay, South America, the competitive market environment means that handsets are given away free to new subscribers. Because there is no benefit to be obtained by theft very little takes place and there is no current market for the resale of stolen handsets.

Hijacking calls

One of the rather less prevalent, and therefore less well-known types of fraud is hijacking. Here, a fraudster uses a radio scanner to identify when a bonafide call is being set up. Once authorisation checks are complete, the call is swamped by RF signals which overpower the genuine phone and hijacks control of the voice channel. The fraudster then simply drops the original call leg and makes his own.

Other illegal activities in the cellular arena include the dandestine recording of private conversations and selling the contents to news media. (As apparently happened to the late Diana, Princess of Wales in the UK and, more recently, to a government minister in Argentina).

Although such activities do not impact operator revenues, they do get high-profile media coverage - which damages operator credibility, increases churn and can even hit the share price.

Fighting back

Having read this litany of horror, you might think that the odds are heavily stacked against cellular operators. And you would be right. This is a game of percentages and there are several steps that operators can take to shave down revenue losses to more acceptable levels.

Ericsson, one of the world's biggest and most prestigious cellular infrastructure and handset manufacturers has devised a list of anti-cloning preventative measures; they include:

* ESN screening: comparison of the transmitted ESN with black-listed numbers, which can prevent a system from providing service to visitors whose ESN matches that of a serial number known to be stolen or fraudulent. If a match is detected, the caller is either disconnected or re-routed;

* MIN screening: comparison of the transmitted MIN with the national numbering format whenever a terminal tries to access an MSC. If the two numbers don't match, access is denied;

* Post-call validation: monitoring of call records, resulting in the removal of invalid phone numbers from service;

* Pre-call validation: the use of IS-41 signalling protocols to query MINESN combinations during call set-up;

* Pulling a switch out of service: a final sanction is to remove from service all the MINs within a given number range, for legitimate or cloned subscribers alike;

* Pulling a service: a doomsday measure to block a frequently abused service, typically international;

* Personal identification numbers (PIN): the use of a PIN for each call made, or for the first call made outside the home catchment area, is an effective short term counter measure to cloning fraud. Although unpopular with subscribers, it allowed one operator to reduce revenue losses attributable to cloning by 70%.

PINs can be used for other applications. They can also give subscribers the option of turning mobile cellular accounts on and off within certain catchment areas; to challenge callers attempting to make calls to international destinations or premium rate numbers; and to require users to validate themselves whenever clone use is suspected or whenever a subscriber terminal has not been used for some time.

However, PINs can be subjected to insider fraud. To reduce the chances of this, the A-key (or private key) is issued and forwarded to the subscriber in a secure manner. This usually involves sending the number in several stages through the post. PIN code masking can be used to conceal the issued PIN number from the subscriber data printout, thereby reducing the risk of insider operator fraud.

The military option

Much current activity in the fight against cloning fraud is in authentication. Variations of this technique,which checks the validity of a calling station, have been used in military voice networks for 50 years. The radio equivalent uses demand-response analysis - a technique which requires the base station to send out an authentication code to a handset, which then responds with a corresponding sequence code.

The identity of a mobile terminal is not automatically accepted simply because its MIN, ESN or PIN are correct. Using cellular authentication and voice encryption (CAVE) algorithms, which obviate the need to send

confidential data over the air interface, the network authentication centre (AC) issues a challenge via the MSC to the calling terminal. To respond to the challenge, the handset must perform calculations using secret embedded data.

Authentication can be used in several different ways:

* Global challenging: used during the system access phase of a call, it requires the calling terminal to execute the CAVE algorithm using the private Akey, details of which are only stored in the terminal and the AC;

* Unique challenging: this is initiated by the AC, which validates the call using data sets stored only inside the calling terminal either on call set-up or upon receipt of a flash request;

* Base station validation: allows the terminal to **validate** the **base station** which is polling it, thereby protecting it against fraudulent attacks;

* Shared secret data (SSD) updating: this involves checking the SSD on a routine or per demand basis;

* Voice privacy: involves the encryption of a subscriber's transmitted conversation on digital networks (the more powerful systems use a combination of TDMA and CAVE);

* Signalling message encryption: protects key subscriber information by encrypting a select sub-set of signalling messages between the base station and terminal.

Authenticate the positive...

All second generation digital phones, as well as a large number of analogue phones, support authentication methods. As the user base of old phones shrinks, those that are susceptible to cloning will also decrease, making fraud more apparent to the operators. The effectiveness of authentication techniques could also be increased by rationalising numbering systems so that all non-authentication compatible models fall within the same number range.

Furthermore, the widespread use of authentication techniques will help limit fraud to subscription swindles and straightforward theft, both of which are more easily identified and prevented than cloning - at least for now.

A number of measures to detect fraudulent activity are built into ACs and MSCs. These are based on activities or service requests associated with a subscriber terminal that is identified as already being in service, or when various technical parameters are exceeded. These include control channel capability, control channel mode mismatch or premature registration. The network will tear down all such calls except for those connected to customer control centres or to the emergency services.

The use of pre-paid cellular accounts also seems to help minimise certain types of billing fraud. However, this solution is unpopular with law enforcement agencies because prepayment for airtime makes it very difficult and expensive to track down individual users. The leader of one big telco investigation unit told CI that his side of the cellular industry "wishes they simply weren't available".

However, their use is on the increase. For example, 46% of this year's new subscribers to Vodafone's UK GSM network have opted for prepayment. It makes it easier for users to manage their spending on mobile calling and helps operators to reduce the amount of bad debt.

...and eliminate the negative

Cellular fraud costs vast sums of money, but controlled measures against it can never be more than partially successful. This is a game of percentage savings.

Furthermore, fraud operators want to retain subscriber confidence, minimise churn and avoid any adverse publicity that might affect market share or stock prices. Thus, they often waive disputed charges or settle out-of-court in return for non-disclosure agreements.

In the end though, it is the honest subscribers who, through paying the higher subscription, connection and call charges that fraud causes, foot the bill for being ripped-off.

Annual losses by Venezuelan cellular operator Telcel are known to be in excess of US$1.5 million. The problem is that Venezuela lies across the Bay of Mexico from Miami, Florida, where it is possible, and completely

legal, to buy cloning kits - complete with instruction manual - on the open market for about $1,500.

One afternoon in 1995, US cops set up impromptu road blocks in New York's Bronx district and challenged motorists with mobile phones to name the carrier service to which they subscribed and how much they paid per month. Several dozen stolen phones were recovered in the short operation.

Few fraud prevention methods are fool-proof, especially the logic-based systems which use the parameters of distance and time between calls from the same subscriber number to detect fraudulent use. Thus, a British fighter pilot who flew down to England from a base in Scotland recently found himself unable to tell his family that he had arrived safely - the cellular operator's software logic had decided that it was impossible for anyone to drive the distance in such a short time and barred his calls.

Some 40% of all car break-ins in London involve the theft of a mobile phone. In other areas of the UK, this figure is even higher. Insurance against theft is available, but at up to US$90 per year many users regard this as too expensive, particularly when the phone itself costs much less than that.

7/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02319693 SUPPLIER NUMBER: 55364093 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Correction: China's Falun Gong War Explodes Onto The Internet 08/03/99 >BY Martyn Williams.
Newsbytes, NA
August 3, 1999
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 775 LINE COUNT: 00069

... addresses used to attack his site were registered to telephone numbers in Beijing. The numbers were, the **AP** said, **verified** as belonging to the Internet Monitoring Bureau of the Public Security Ministry.
Other media reports quoted Webmasters...

7/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02318821 SUPPLIER NUMBER: 55346996 (USE FORMAT 7 OR 9 FOR FULL TEXT)
******Falun Gong War Explodes Onto Internet - Update 08/02/99 >BY David McGuire.**
Newsbytes, NA
August 2, 1999
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 750 LINE COUNT: 00066

... addresses used to attack his site were registered to telephone numbers in Beijing. The numbers were, the **AP** said, **verified** as belonging to the Internet Monitoring Bureau of the Public Security Ministry.
Other media reports quoted Webmasters...

7/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02318798 SUPPLIER NUMBER: 55346973 (USE FORMAT 7 OR 9 FOR FULL TEXT)
China's Falun Gong War Explodes Onto The Internet 08/02/99 >BY Martyn Williams.
Newsbytes, NA
August 2, 1999
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 600 LINE COUNT: 00054

... Internet addresses used to attack his site were registered to telephone numbers in Beijing which were, the **AP** said, **verified** as belonging to the Internet Monitoring Bureau of the Public Security Ministry.
Other media reports quoted Webmasters...

7/3,K/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02268484 SUPPLIER NUMBER: 53851436 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Boardtek Receives Rambus PC Board Order from Intel 02/08/99.
Newsbytes, NA
Feb 9, 1999

LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 126 LINE COUNT: 00014

TEXT:
...nearly two years. Most Taiwanese Rambus interface PC Board manufacturers send their products to Boardtek for Rambus **validation** . **AP** Acer Technology Inc. and Kingmax Technology Inc. are also major manufacturers in Taiwan that produce Rambus interface...

7/3,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

01918543 SUPPLIER NUMBER: 18150175 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Digital Pathways' Windows NT Security Server.
Newsbytes, pNEW04020021
April 2, 1996
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 431 LINE COUNT: 00039

... protocol) and remote log-on services, and eliminates the need to install proprietary hardware at each network **access point** .
According to Tankard, users are **authenticated** through one-time passwords generated by the DSS NT and SecureNet Key tokens. DSS NT supports standards...

7/3,K/6 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

01318147 SUPPLIER NUMBER: 07894668 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Fast file service with DFS. (Distributed File Services)
Verkade, Herman
DEC User, p59(2)
Sept, 1989
ISSN: 0263-6530 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2503 LINE COUNT: 00182

... is accessed. However, when mounting an access point, a DNS server must be reachable in order to **validate** the **access point** . When multiple files are accessed, DFS multiplexes requests to the same node over a single link to...

7/3,K/7 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2005 The Gale Group. All rts. reserv.

01784999 Supplier Number: 53533767 (USE FORMAT 7 FOR FULLTEXT)
SSH Communications Security Delivers Standards-based Virtual Private Networking (VPN) Cryptographic Security to Xedia Corporation.
PR Newswire, p0630
Jan 8, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 476

... management and authentication into IPSec based networking devices. It supports the Internet Key Exchange (IKE) which automatically **authenticates** the **Access Point** QVPN and clients connecting to it. It also negotiates the security policy and encryption keys in a...

7/3,K/8 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2005 The Gale Group. All rts. reserv.

01726104 Supplier Number: 53074197 (USE FORMAT 7 FOR FULLTEXT)
Xedia Unveils Performance Results from Competitive Evaluation with Cisco.
PR Newswire, p9219
Oct 12, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 579

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
Acces s Point 's Precise Bandwidth Management **Validated**

7/3,K/9 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2005 The Gale Group. All rts. reserv.

01679226 Supplier Number: 50177990 (USE FORMAT 7 FOR FULLTEXT)
HP Introduces W-CDMA Code-Domain Power Measurement Software to Aid Development of 3G Base Stations; First Solution Successfully Demonstrated at NTT DoCoMo, Japan.
Business Wire, p07200181
July 20, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Newswire; Trade
Word Count: 556

... CDMA base stations by using the new software with the HP 89400 series vector signal analyzer to **verify** that **base - station** systems transmit correct coding for all symbol rates.
NTT DoCoMo, a leading mobile communications operator in Japan...

7/3,K/10 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2005 The Gale Group. All rts. reserv.

01426812 Supplier Number: 46710384 (USE FORMAT 7 FOR FULLTEXT)
LeeMah DataCom Introduces SafeAccess Server For Scaleable Enterprise Network Security.
Business Wire, p09160498
Sept 16, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 630

... access to network information and resources.
Based on Data Encryption Standard (DES) algorithms for challenge/response user **authentication** and **access point** protection, SafeAccess protects the network at the point of access, before a user can gain access to...

7/3,K/11 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

04396534 Supplier Number: 55347002 (USE FORMAT 7 FOR FULLTEXT)
******Falun Gong War Explodes Onto Internet - Update 08/02/99 >BY David McGuire Martyn Williams.**

Newsbytes, pNA
August 2, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; General Trade
Word Count: 755

... addresses used to attack his site were registered to telephone numbers in Beijing. The numbers were, the **AP** said, **verified** as belonging to the Internet Monitoring Bureau of the Public Security Ministry.
Other media reports quoted Webmasters...

7/3,K/12 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

03884938 Supplier Number: 48492842 (USE FORMAT 7 FOR FULLTEXT)
FTP SOFTWARE: FTP Software introduces 'on-demand' host applications for Windows and the Web
M2 Presswire, pN/A
May 21, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 587

... administrators can now centralise policy (session files) for multiple platforms and control users with a single, secure **access point**.
The **authenticated** user is delivered a personalised Web page that presents the host applications that are available to them...

7/3,K/13 (Item 3 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

03337957 Supplier Number: 46860801 (USE FORMAT 7 FOR FULLTEXT)
PERICOM: Pericom announces Periflex - A new concept in support services
M2 Presswire, pN/A
Nov 4, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 612

... Recovery Planning. Pericom will design and instigate a full disaster recovery strategy.
Security Cheek. Fileservers, workstations and **access points** will all be **validated** and investigated for possible breaches of security.
Emergency Help Desk - Instant support as and when required, no...

7/3,K/14 (Item 4 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

03174630 Supplier Number: 46507207 (USE FORMAT 7 FOR FULLTEXT)
DIGITAL PATHWAYS: Digital Pathways' Defender Security Server wins 'Best Remote Dial-up Access Control' product award
M2 Presswire, pN/A
July 1, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 629

... FTP and remote log-on services and eliminates the need to install proprietary hardware at each network **access point** .
Users are **authenticated** through one-time passwords generated by the DSS NT and SecureNet Key tokens, providing a consistent, easy...

7/3,K/15 (Item 5 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03073012 Supplier Number: 46278448 (USE FORMAT 7 FOR FULLTEXT)
Digital Pathways' Windows NT Security Server 04/02/96
Newsbytes, pN/A
April 2, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; General Trade
Word Count: 400

... protocol) and remote log-on services, and eliminates the need to install proprietary hardware at each network **access point** .
According to Tankard, users are **authenticated** through one-time passwords generated by the DSS NT and SecureNet Key tokens. DSS NT supports standards...

7/3,K/16 (Item 6 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03056884 Supplier Number: 46244933 (USE FORMAT 7 FOR FULLTEXT)
DIGITAL PATHWAYS: Digital Pathways announces first security server on Windows NT
M2 Presswire, pN/A
March 25, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 566

... FTP and remote log-on services and eliminates the need to install proprietary hardware at each network **access point** .
Users are **authenticated** through one-time passwords generated by the DSS NT and SecureNet Key tokens.
DSS NT supports standards...

7/3,K/17 (Item 7 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

01890606 Supplier Number: 43278184 (USE FORMAT 7 FOR FULLTEXT)
SCS Mobilecom Submits B-CDMA to TIA for Standardization
PCS News, v3, n18, pN/A
Sept 3, 1992
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 161

... the attributes of B-CDMA and to establish whether Cox's cable distribution network could link PCS **base stations** . The tests **validated** the performance of three key elements in the development of a B-CDMA system, including: the base...

7/3,K/18 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

(c) 2005 The Gale Group. All rts. reserv.

06809688 Supplier Number: 56910350 (USE FORMAT 7 FOR FULLTEXT)
Testing on a Budget.
Pahls, Jason W. Gallo & Mary Jane
Wireless Review, pNA
Sept 30, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1248

... in some significant way, technicians will need to run a suite of acceptance or commissioning tests to **verify** the **base station** still is operating correctly. Automated testing accomplishes this task with speed and efficiency.
MEASUREMENT REPEATABILITYAlthough easy, efficient...

7/3,K/19 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

05812956 Supplier Number: 50318613 (USE FORMAT 7 FOR FULLTEXT)
W-CDMA test solutions
Telephony, pNA
Sept 7, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Magazine/Journal; Trade
Word Count: 82

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...develop W-CDMA base stations. The system consists of new software and a vector signal analyzer that **verifies** that **base station** systems transmit correct coding for all symbol rates. The HP 89441 vector signal analyzer costs $67,580...

7/3,K/20 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

03977202 Supplier Number: 45771708 (USE FORMAT 7 FOR FULLTEXT)
Obstacle course
Flight International, p36
Sept 6, 1995
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2427

... the US Federal Aviation Administration for more than two years to sign a bilateral airworthiness agreement. Mutual **verification** of **AP** -23/FAR-23 regulations is being made, using the four-seat, low-wing, Ilyushin Il-103 as...

7/3,K/21 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

02277840 Supplier Number: 42977747 (USE FORMAT 7 FOR FULLTEXT)
Rohde & Schwarz wins testing deal
Electronics Times, p2
May 7, 1992

Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 33

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...from the French second operator for gsm radio telephones to supply an intermediate base station tester to **validate base stations** being supplied by Alcatel and PKI.

7/3,K/22 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

10284330 SUPPLIER NUMBER: 20805059 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Air raid warnings. (fraud in the cellular telephone business)
Wittering, Stewart; Daniels, Guy; Warwick, Martyn
Communications International, v25, n5, p47(5)
May, 1998
ISSN: 0305-2109 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 3550 LINE COUNT: 00281

... call set-up or upon receipt of a flash request;
* Base station validation: allows the terminal to **validate** the **base station** which is polling it, thereby protecting it against fraudulent attacks;
* Shared secret data (SSD) updating: this involves...

7/3,K/23 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

10254133 SUPPLIER NUMBER: 20788425 (USE FORMAT 7 OR 9 FOR FULL TEXT)
SecureNetworx Breaks the Price Barrier With "Strong Authentication" DigitalTokens.
Business Wire, p6150023
June 15, 1998
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 843 LINE COUNT: 00082

... based upon individual or group attributes and restrictions, including: -0-
-- PAP authentication
-- CHAP authentication
-- Digital Token strong **authentication**
-- Network **access point**
-- Login attempts
-- Password expiration
-- Simultaneous session limits
-- Day-date-time restrictions
-- Maximum sessions-per-day
Support for...

7/3,K/24 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

09830235 SUPPLIER NUMBER: 17762494 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Power amplifier spectral regrowth for digital cellular and PCS applications. (personal communication services)
Kenney, J. Stevenson; Leke, Achankeng
Microwave Journal, v38, n10, p74(10)

Oct, 1995
ISSN: 0192-6225 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 4616 LINE COUNT: 00391

TEXT:
...performed to calculate spectral regrowth, and the power is integrated over a channel bandwidth to obtain the **AP** . The model is **verified** by comparing its results with the measured ACP from a two-stage 1.9 GHz GaAs radio...

7/3,K/25 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

09656658 SUPPLIER NUMBER: 19319924 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Single card access moves into the future. (colleges and universities)
Fickes, Michael
School Planning and Management, v36, n2, p26F(2)
Feb, 1997
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 851 LINE COUNT: 00074

... illuminated red and green panel lights indicating access restrictions and permissions.
A hand geometry scanner at each **access point** also **verified** identities, according to Robert Lang, who managed the project for Georgia Tech. "Once the hand was inserted...

7/3,K/26 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

09309312 SUPPLIER NUMBER: 18850261 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Back to Beirut.(former hostage Terry Anderson returns to Lebanon)
Cohen, Jodi B.
Editor & Publisher, v129, n42, p12(2)
Oct 19, 1996
ISSN: 0013-094X LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1706 LINE COUNT: 00130

... it at that point would have been sticking our heads in the sand."
After its first report, **AP verified** the information with its own law enforcement sources, Christian added.
"This obviously became a stampede, and I...

7/3,K/27 (Item 6 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

08848801 SUPPLIER NUMBER: 18545114
The cataloging practices of special libraries and their relationship with OCLC. (Online Computer Library Center)
Hsieh-Yee, Ingrid
Special Libraries, v87, n1, p10(11)
Wntr, 1996
ISSN: 0038-6723 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4280 LINE COUNT: 00391

... reviewed the description of the records and more than 33 percent verified the main entries. Efforts to **verify access points** are justified because they are important for retrieval. However, the review of descriptive cataloging provided by the...

7/3,K/28 (Item 7 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

08162103 SUPPLIER NUMBER: 17493253 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Obstacle course: Russian GA manufacturers chafe at the bit at slow progress being made in the country's industry. (general aviation)
Velovich, Alexander
Flight International, v148, n4488, p36(3)
Sep 6, 1995
ISSN: 0015-3710 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2602 LINE COUNT: 00204

... the US Federal Aviation Administration for more than two years to sign a bilateral airworthiness agreement. Mutual **verification** of **AP** -23/FAR-23 regulations is being made, using the four-seat, low-wing, Ilyushin Il-103 as...

7/3,K/29 (Item 8 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

07610807 SUPPLIER NUMBER: 16562780 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Testing PDH traffic on SDH networks. (Synchronous Digital Hierarchy) (includes related article)
Rice, Robert
Communications International, v21, n11, p57(2)
Nov, 1994
ISSN: 0305-2109 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1707 LINE COUNT: 00136

... rates, and high SDH BIP and PDH CRC error conditions. Lastly, the element's automatic protection switching (**APS**) capability should be **verified** by using the test instrument to transmit stressful line conditions, and by monitoring the element switch over...

7/3,K/30 (Item 9 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

07547904 SUPPLIER NUMBER: 15784645 (USE FORMAT 7 OR 9 FOR FULL TEXT)
No TRO for Ad/Sat. (temporary restraining order; electronic advertising-delivery service) (Editorial)
Giobbe, Dorothy
Editor & Publisher, v127, n40, p11(2)
Oct 1, 1994
DOCUMENT TYPE: Editorial ISSN: 0013-094X LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 994 LINE COUNT: 00078

... the judge correctly found that none of the plaintiff's points were correct," Drebsky said. "The decision **validates** **AP** 's position."

7/3,K/31 (Item 10 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.

07493818 SUPPLIER NUMBER: 15643880 (USE FORMAT 7 OR 9 FOR FULL TEXT)
New way to swap engineering data: PlantSTEP comprises a consortium of companies whose goal is to revolutionize information management of

process plants. (group founded on industrial data standard)
Molad, C.
Hydrocarbon Processing, v73, n7, p109(2)
July, 1994
ISSN: 0018-8190 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1267 LINE COUNT: 00109

... development of a prototyping environment for the AP. This environment, or laboratory, will seek to understand and **verify** **AP** implementability during the development phase. Additionally, NIST will provide one part-time person to support the ISO...

7/3,K/32 (Item 11 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

06231306 SUPPLIER NUMBER: 12604476 (USE FORMAT 7 OR 9 FOR FULL TEXT)
How they watch Washington: Newspapers are revamping the way they cover the inside-the-beltway beat.
Bonafede, Dom
Columbia Journalism Review, v31, n3, p35(5)
Sept-Oct, 1992
ISSN: 0010-194X LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1753 LINE COUNT: 00139

... your story is so great, why isn't it on the wires?' They're always looking for **validation** from **AP** , Reuters, or The New York Times."
What competition does exist among the bureaus can have a certain...

7/3,K/33 (Item 1 from file: 624)
DIALOG(R)File 624:McGraw-Hill Publications

0571426
ROSA TESTS BEGIN TO VERIFY AP -600 SAFETY CASE FOR NRC
Naoaki Usui
Nucleonics Week, Vol. 35, No. 18, Pg 15
May 5, 1994
JOURNAL CODE: NUC
ISSN: 0048-105X
WORD COUNT: 332

ROSA TESTS BEGIN TO VERIFY AP -600 SAFETY CASE FOR NRC

7/3,K/34 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01909747 05-60739
Testing on a budget
Gallo, Jason W; Pahls, Mary Jane
Wireless Review v16n18 PP: 70-74 Sep 15, 1999
ISSN: 1097-3893 JRNL CODE: WLR
WORD COUNT: 1333

...TEXT: in some significant way, technicians will need to run a suite of acceptance or commissioning tests to **verify** the **base station** still is operating correctly. Automated testing accomplishes this task with speed and efficiency.

Measurement Repeatability

Although easy...

7/3,K/35 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01318866 99-68262
'Gotcha' gamble
Giobbe, Dorothy
Editor & Publisher v129n42 PP: 8-11 Oct 19, 1996
ISSN: 0013-094X JRNL CODE: EDP
WORD COUNT: 1230

...TEXT: it at that point would have been sticking our heads in the sand."

After its first report, **AP** **verified** the information with its own law enforcement sources, Christian added.

"This obviously became a stampede, and I...

7/3,K/36 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00951104 96-00497
In the mail
Rosenfield, James R
Direct Marketing v57n8 PP: 32-35 Dec 1994
ISSN: 0012-3188 JRNL CODE: DIM
WORD COUNT: 2738

...TEXT: name and address window: "OFFICIAL NOTIFICATION OF GUARANTEED CASH AVAILABILITY THE INFORMATION CONTAINED HEREIN HAS BEEN AUTHORIZED, **VERIFIED** , **AP** -PROVED AND IS FULLY GUARANTEED BY INTERNAL REGULATIONS."

"FULLY GUARANTEED BY INTERNAL REGULATIONS?" It takes your breath...

7/3,K/37 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00549495
iPASS HAS A WORLDWIDE SOLUTION FOR INTERNET MAIL ACCESS
Eric Arnum, Senior Contributing Editor
Wireless Messaging Report
July 8,1997 VOL: 5 ISSUE: 13 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 1186 RECORD TYPE: FULLTEXT

TEXT:
...where their access point is busy. [With iPass] you're able to dial into another provider's **access** **point** , get **authenticated** back to your home ISP, use that access point, and presumably get billed for that usage from ...

7/3,K/38 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire

0932275 BW0226

HEWLETT PACKARD 4: W-CDMA Code-Domain Power Measurement Capability Now Available for HP 89400 Series Vector Signal Analyzer

November 02, 1998

Byline: Computer Writers

...D engineers can accelerate the development of W-CDMA base stations by using this new measurement to **verify** that **base - station** systems transmit correct coding for all symbol rates.

HP has a wide range of design and test...

```
File   8:Ei Compendex(R) 1970-2005/Apr W2
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Mar
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Apr W3
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Apr W2
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Mar W1
         (c)2005 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2005/Apr W2
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Apr W2
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Apr W2
         (c) 2005 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Mar
         (c) 2005 The HW Wilson Co.
File 266:FEDRIP 2005/Jan
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2005/Mar W2
         (c) 2005 FIZ TECHNIK
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 483:Newspaper Abs Daily 1986-2005/Apr 16
         (c) 2005 ProQuest Info&Learning
File 438:Library Lit. & Info. Science 1984-2005/Feb
         (c) 2005 The HW Wilson Co
File 256:TecInfoSource 82-2005/Feb
         (c) 2005 Info.Sources Inc

Set     Items   Description
S1     140360   ACCESS()POINT? ? OR AP OR APS OR BASE()STATION? ? OR WIREL-
              ESS()(ROUTER? ? OR GATEWAY? ?)
S2         59   S1(5W)(AUTHENTICATED OR VALIDATED OR VERIFIED)
S3          0   S1(5W)((AUTHENTICATE OR AUTHENTICATES OR AUTHENTICATING OR
              VALIDATE OR VALIDATES OR VALIDATING)(1W)(ITSELF OR OWN()SELF -
              OR THEMSELVES))
S4         32   (AUTHENTICAT??? OR VALIDAT??? OR VERIF?)(1W)S1
S5        649   MUTUAL?()(AUTHENTICAT??? OR VALIDAT??? OR VERIF?)
S6         12   S1(10N)S5
S7        100   S2 OR S4 OR S6
S8         75   RD (unique items)
S9         43   S8 NOT PY=2001:2005
```

9/5/6 (Item 6 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

02175146 E.I. Monthly No: EI8703022944
Title: PIN VERIFICATION WITH MULTIPLE PERSONAL AUTHENTICATION CODES.
Author: Anon
Source: IBM Technical Disclosure Bulletin v 29 n 5 Oct 1986 p 1924-1927
Publication Year: 1986
CODEN: IBMTAA ISSN: 0018-8689
Language: ENGLISH
Document Type: JA; (Journal Article) Treatment: A; (Applications)
Journal Announcement: 8703
Abstract: This article describes a compartmentalized transaction security facility which is an improvement or refinement on the method described in a previously published paper. The improvement provides a defense against a 'substituted ID' attack by calculating the user's personal authentication code (PAC) as a function of the user's identifier (ID) and **authentication** parameter (**AP**) rather than AP alone. 1 ref.
Descriptors: *DATA PROCESSING, BUSINESS--*Security of Data; BUSINESS MACHINES
Identifiers: PIN VERIFICATION; AUTHENTICATION CODES; TRANSACTION SECURITY ; USER'S IDENTIFIER; AUTHENTICATION PARAMETER
Classification Codes:
723 (Computer Software); 722 (Computer Hardware); 912 (Industrial Engineering & Management)
72 (COMPUTERS & DATA PROCESSING); 91 (ENGINEERING MANAGEMENT)

9/5/7 (Item 7 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01544402 E.I. Monthly No: EI8407064258 E.I. Yearly No: EI84031501
Title: UNIFIED AUTHENTICATION PARAMETER.
Author: Matyas, S. M.; Meyer, C. H.; Oseas, J.
Source: IBM Technical Disclosure Bulletin v 26 n 7A Dec 1983 p 3284-3285
Publication Year: 1983
CODEN: IBMTAA ISSN: 0018-8689
Language: ENGLISH
Journal Announcement: 8407
Abstract: A method is reported for generating an **authentication** parameter (**AP**). It may be used for personal verification, as a function of user-remembered secret information, namely, a personal identification number (PIN) in combination with additional static information.
Descriptors: *DATA PROCESSING--*Security of Data
Identifiers: AUTHENTICATION PARAMETERS
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

9/5/8 (Item 8 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01542202 E.I. Monthly No: EI8407064257 E.I. Yearly No: EI84031500
Title: COUPLING PAC TO BOTH AP AND ID.
Author: Lennon, R. E.; Matyas, S. M.; Meyer, C. H.; Oseas, J.
Source: IBM Technical Disclosure Bulletin v 26 n 6 Nov 1983 p 2803-2805
Publication Year: 1983
CODEN: IBMTAA ISSN: 0018-8689
Language: ENGLISH
Journal Announcement: 8407
Abstract: A user verification process is described which depends on

several related input parameters, namely, a user identifier (ID), an **authentication** parameter (**AP**) and a personal authentication code (PAC). Use of a system is denied to users unless the correct correspondence between ID, AP and PAC can be demonstrated.
Descriptors: *DATA PROCESSING--*Security of Data
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

9/5/15 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

5305531 INSPEC Abstract Number: B9608-6250F-028
Title: Verification of authentication protocol for CDMA mobile communication network
Author(s): Ki-Yoong Hong; Seok-Woo Kim; Dong-Kyoo Kim
Journal: Journal of Electrical Engineering and Information Science vol.1, no.1 p.82-90
Publisher: Korean Inst. Electr. Eng,
Publication Date: March 1996 Country of Publication: Taiwan
ISSN: 1226-1262
SICI: 1226-1262(199603)1:1L.82:VAPC;1-1
Material Identity Number: F212-96001
Language: English Document Type: Journal Paper (JP)
Treatment: Applications (A); Practical (P); Theoretical (T)
Abstract: We present an analysis of the IS-95 authentication protocol for the code division multiple access (CDMA) mobile communication network. We propose a **mutual authentication** protocol, **AP** -6, to improve the security and correctness. Formal description and verification of the proposed AP-6 are also presented on the basis of the formal logic. It is shown that the proposed AP-6 is more secure and correct than the IS-95 authentication protocol. (8 Refs)
Subfile: B
Descriptors: code division multiple access; formal logic; formal verification; land mobile radio; message authentication; radio networks
Identifiers: authentication protocol verification; CDMA mobile communication network; IS-95 authentication protocol; code division multiple access; AP-6; security; formal description; formal verification; formal logic
Class Codes: B6250F (Mobile radio systems); B6150E (Multiple access communication); B6150M (Protocols)

9/5/20 (Item 8 from file: 2)
DIALOG(R)File 2:INSPEC

02254234 INSPEC Abstract Number: C84027070
Title: Strengthening authentication patterns
Author(s): Hopkins, W.D.; Lennon, R.E.; Matyas, S.M.; Meyer, C.H.
Author Affiliation: IBM Corp., Armonk, NY, USA
Journal: IBM Technical Disclosure Bulletin vol.26, no.8 p.4121-2
Publication Date: Jan. 1984 Country of Publication: USA
CODEN: IBMTAA ISSN: 0018-8689
Language: English Document Type: Journal Paper (JP)
Treatment: Applications (A); New Developments (N); Practical (P)
Abstract: Discloses a method for strengthening **authentication** patterns (**AP**) used as part of a personal verification process in an electronic funds transfer (EFT) system. (0 Refs)

```
File 348:EUROPEAN PATENTS 1978-2005/Apr W02
         (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050414,UT=20050407
         (c) 2005 WIPO/Univentio

Set     Items   Description
S1      40563   ACCESS()POINT? ? OR BASE()STATION? ? OR WIRELESS().(ROUTER?
             ? OR GATEWAY? ?)
S2         84   S1(5W)(AUTHENTICATED OR VALIDATED OR VERIFIED)
S3          7   S1(5W)((AUTHENTICATE OR AUTHENTICATES OR AUTHENTICATING OR
             VALIDATE OR VALIDATES OR VALIDATING)(1W)(ITSELF OR OWN()SELF -
             OR THEMSELVES))
S4        120   (AUTHENTICAT??? OR VALIDAT??? OR VERIF?)(1W)S1
S5       1149   (MUTUAL? OR BIDIRECTIONAL OR BI()DIRECTIONAL)()(AUTHENTICA-
             T??? OR VALIDAT??? OR VERIF? OR CHECK???)
S6         25   S1(10N)S5
S7        191   S2:S4 OR S6
S8        140   S7 AND AC=US/PR
S9         61   S8 AND AY=(1970:1999)/PR
S10        57   S7 AND PY=1970:1999
S11        76   S9:S10
```

11/3,K/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01634639
PCS pocket phone/microcell communication over-air protocol
PCS-Taschentelefon/Mikrozellen Funkubertragungsprotokoll
Protocole hertzien de communications pour telephone portable ou systeme micro-cellulaire
PATENT ASSIGNEE:
XIRCOM Wireless, Inc., (3959270), 1365 Garden of the Gods Road, Colorado Springs, Colorado 80907, (US), (Applicant designated States: all)
INVENTOR:
Anderson, Gary B., 4535 North Lake Boulevard, Carnelian Bay, CA 95711, (US)
Jensen, Ryan N., 4510 Sleepy Hollow, Colorado Springs, CO 80917, (US)
Petch, Bryan K., 5925 Del Ray Drive, Colorado Springs, CO 80918, (US)
Peterson, Peter O., 630D Autumn Crest Circle, Colorado Springs, CO 80919, (US)
LEGAL REPRESENTATIVE:
Leeming, John Gerard (74731), J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5JJ, (GB)
PATENT (CC, No, Kind, Date): EP 1347658 A2 030924 (Basic)
EP 1347658 A3 040303
APPLICATION (CC, No, Date): EP 2003014441 950320;
PRIORITY (CC, No, Date): US 215306 940321; US 284053 940801
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 763300 (EP 95914135)
INTERNATIONAL PATENT CLASS: H04Q-007/20
ABSTRACT WORD COUNT: 190
NOTE:
Figure number on first page: 1-1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200339	265
SPEC A	(English)	200339	53905
Total word count - document A			54170
Total word count - document B			0
Total word count - documents A + B			54170

...SPECIFICATION and selects antennas for space diversity and polarization when appropriate, as well as controls the MS power.
Authentication . The **Base Station** responds to Notes from the Base Station Controller to authenticate a given MS. The BS sends the...

11/3,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01250947
Secure wireless local area network
Gesichertes drahtloses lokales Netzwerk
Reseau local radio securise
PATENT ASSIGNEE:
INTEL CORPORATION, (322932), 2200 Mission College Boulevard, P.O. Box 58119, Santa Clara, CA 95052-8119, (US), (Applicant designated States: all)
INVENTOR:
Weatherspoon, Sultan, 16410 N.E. 32nd St., Vancouver, WA 98682, (US)
Glendinning, Duncan, 1840 W. Azalea Dr., Chandler, AZ 85248, (US)

LEGAL REPRESENTATIVE:
Botti, Mario (87642), Botti & Ferrari S.r.l. Via Locatelli, 5, 20124 Milano, (IT)
PATENT (CC, No, Kind, Date): EP 1081895 A1 010307 (Basic)
APPLICATION (CC, No, Date): EP 103334 000221;
PRIORITY (CC, No, Date): US 389437 990903
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-012/28; H04L-029/06
ABSTRACT WORD COUNT: 247
NOTE:
Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200110	620
SPEC A	(English)	200110	2653
Total word count - document A			3273
Total word count - document B			0
Total word count - documents A + B			3273

...ABSTRACT The AP transmits the first and second authentication messages to the authentication server. If the authentication server **validates** the **access point** and the operator's logon name and password, it will authorize access to the wired network.

...SPECIFICATION is connected to the wired LAN for providing the operator with access to the wired LAN after **authenticating** the **access point** , the wireless device, and the operator.
Brief description of the drawings
The foregoing and other objects, features...

...CLAIMS server connected to the wired LAN for providing the operator with access to the wired LAN after **authenticating** the **access point** , the wireless device, and the operator.
2. The secure wireless LAN of claim 1 wherein the access...

...transmitting the first authentication message from the access point to a wireless device over a wireless channel;
validating the **access point** by analyzing the first authentication message;
generating a second authentication message including validating information about the wireless...

...analyzing the second authentication message;
transmitting the first and second authentication messages to an authentication server after **validating** the **access point** and the wireless device;
validating the operator; and
enabling a data channel between the wireless device and other devices on the wired LAN after **validating** the **access point** and the operator.
9. The method of claim 8 wherein transmitting the first authentication message includes transmitting...

11/3,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01029460
Method for conflict resolution in a multiple acess system for communications networks

Verfahren zur Konfliktauflosung in einem Vielfachzugriffssystem fur Kommunikationsnetze
Methode pour resoudre des conflicts dans un systeme d'acces multiple pour reseaux de communication
PATENT ASSIGNEE:
LUCENT TECHNOLOGIES INC., (2143720), 600 Mountain Avenue, Murray Hill, New Jersey 07974-0636, (US), (applicant designated states: AT;BE;CH;CY;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Chuah, Mooi Choo, 184B Eatoncrest Drive, Eatontown, New Jersey 07724, (US)
LEGAL REPRESENTATIVE:
Watts, Christopher Malcolm Kelway, Dr. et al (37391), Lucent Technologies (UK) Ltd, 5 Mornington Road, Woodford Green Essex, IG8 0TU, (GB)
PATENT (CC, No, Kind, Date): EP 917317 A1 990519 (Basic)
APPLICATION (CC, No, Date): EP 98308333 981013;
PRIORITY (CC, No, Date): US 61790 P 971014; US 77741 P 980312; US 83677 980522
DESIGNATED STATES: DE; FR; GB; IT; SE
INTERNATIONAL PATENT CLASS: H04L-012/28;
ABSTRACT WORD COUNT: 330

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9920	1390
SPEC A	(English)	9920	22037
Total word count - document A			23427
Total word count - document B			0
Total word count - documents A + B			23427

...SPECIFICATION of stations:
1. Whenever a reassociate request frame is received from a station and the station is **authenticated** , the **access point** transmits a reassociation response with a status value indicating "successful";
2. If the status value is "successful...

11/3,K/16 (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01005296
MOBILE COMMUNICATION METHOD AND MOBILE COMMUNICATION SYSTEM
MOBILES KOMMUNIKATIONSVERFAHREN UND ANORDNUNG
PROCEDE ET SYSTEME DE COMMUNICATION MOBILE
PATENT ASSIGNEE:
NTT MOBILE COMMUNICATIONS NETWORK INC., (1560153), 10-1, Toranomon 2-chome, Minato-ku, Tokyo 105-8436, (JP), (Applicant designated States: all)
INVENTOR:
TAMURA, Motoshi, 18-2-101, Nobi 4-chome Yokosuka-shi, Kanagawa 239-0841, (JP)
MIKI, Mutsumaru, 18-2-105, Nobi 4-chome Yokosuka-shi, Kanagawa 239-0841, (JP)
OKAMOTO, Akiko Green Gables C-101,12-14, Tokuyoshi Higashi 1-chome, Kokura, Minami-ku, Kitakyusyu-shi, Fukuoka 803-0277, (JP)
KUSUNOSE, Kenya, 6-1-302, Hikarinooka Yokosuka-shi, Kanagawa 239-0847, (JP)
UCHIKOSHI, Akihiro, 18-2-304, Nobi 4-chome Yokosuka-shi, Kanagawa 239-0841, (JP)
IGARASHI, Daisuke, 6-1-508, Hikarinooka Yokosuka-shi, Kanagawa 239-0847, (JP)
YAMAGATA, Katsuhiko, 1-22-3-302, Kosugaya Sakae-ku Yokohama-shi, Kanagawa 247-0007, (JP)

SATO, Takaaki, 18-4-704, Nobe 4-chome, Yokosuka-shi Kanagawa 239-0841, (JP)
HAGIWARA, Junichiro, Adorabure Kuriki A-101, 2-35-3, Kuriki, Isogo-ku, Yokohama-shi Kanagawa 235-0041, (JP)
WATANABE, Yasuyuki, 18-4-603, Nobi 4-chome, Yokosuka-shi, Kanagawa 239-0841, (JP)
HAMAJIMA, Takuya, 606, Marine Heim 1283-3, Tauraminato-cho, Yokosuka-shi Kanagawa 237-0071, (JP)
HATA, Masafumi, 3-301 Daikan Plaza City 1-8, Yasuura-cho, Yokosuka-shi Kanagawa 238-0012, (JP)
ISHIKAWA, Nobutaka 202, Bell Light Nokendai, 18-11, Nokendai-tori Kanazawa-ku Yokohama-shi, Kanagawa 236-0053, (JP)
YASUDA, Yoshiyuki, 6-13-31, Okamura Isogo-ku Yokohama-shi, Kanagawa 235-0021, (JP)
YUNOKI, Kazufumi, 18-4-304, Nobi 4-chome Yokosuka-shi, Kanagawa 239-0841, (JP)
UCHIYAMA, Nobuhide, 20-1-201, Yoshimien 9-chome, Sacki-ku, Hiroshima-shi, Hiroshima 731-5132, (JP)
LEGAL REPRESENTATIVE:
HOFFMANN - EITLE (101511), Patent- und Rechtsanwalte Arabellastrasse 4, 81925 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 978958 A1 000209 (Basic)
WO 9848528 981029
APPLICATION (CC, No, Date): EP 98917680 980424; WO 98JP1906 980424
PRIORITY (CC, No, Date): JP 97123782 970424
DESIGNATED STATES: DE; FR; GB; IT; SE
INTERNATIONAL PATENT CLASS: H04B-007/26; H04Q-007/24
ABSTRACT WORD COUNT: 244
NOTE:
Figure number on first page: 226

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200006	7277
SPEC A	(English)	200006	100683
Total word count - document A			107960
Total word count - document B			0
Total word count - documents A + B			107960

...SPECIFICATION mobile communication including a mobile station which is able to conduct diversity reception, a plurality of radio **base stations** , and a base station controller communicating via the radio base stations under control of a switching center...

...mobile communication including a mobile station which is able to conduct diversity reception, a plurality of radio **base stations** , and a base station controller communicating via the radio base stations under control of a switching center...trigger requirement to TACF triggers the handover. Then, the network selects the base station among the candidate **base stations** in order to execute the handover and notifies the mobile station MS about the selected base station, thereby activating the traffic channel in relation to the **base station** . Accordingly, it is possible for the network to exclude complicated control procedures, e.g., detection procedure of...mobility management.

With such a structure, prior to the mutual notification of the encipherment onset, a user **authentication** procedure (refer to section 2.4.5.1) is executed as shown in Figure 63. In execution of the user **authentication** procedure, a certificated encipherment key is previously stored at UIMF and LRDF of the network and mobile...arithmetic operation based on the authentication information (random number) and transmits the authentication calculation result as an **authentication** response at step S4. The authentication calculation uses an authentication key stored in each mobile station MS...for recognition.

c) The user authentication of the mobile station is executed as

described above. The user **authentication** will be described in more detail at the section entitled "User Authentication" of this chapter.

d) In...calling and destination user terminals. "Incoming call acceptance" procedures include paging, SDCCH control, user identity retrieval, user **authentication** , encipherment-onset time notification, routing in the network, establishment of access link, mutual information transfer to and...

...can respond to another call (additional call). However, since the mobile terminal has been already authenticated, the **authentication** process is not carried out for the additional call.

Furthermore, if a plurality of mobile stations respond...directed to a mobile station, or when the location is registered.

In order to execute the user **authentication** , the system comprises the following capabilities.

When a mobile station accesses the network, the network produces various...

11/3,K/17 (Item 17 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01001689
Cellular telephony authentication arrangement
Authentifizierungsvorrichtung fur zellulare Telefone
Dispositif d'authentification pour la telephonie cellulaire
PATENT ASSIGNEE:
AT&T Corp., (589370), 32 Avenue of the Americas, New York, NY 10013-2412, (US), (Proprietor designated states: all)
INVENTOR:
Reeds III, James Alexander, 127 Southgate Road, New Providence, New Jersey 07974, (US)
Treventi, Philip Andrew, 15 Candlewood Drive, Murray Hill, New Jersey 07974, (US)
Yu, I-Hsiang, 9 Hickory Place, Cedar Knolls, New Jersey 07927, (US)
LEGAL REPRESENTATIVE:
Buckley, Christopher Simon Thirsk et al (28912), Lucent Technologies (UK) Ltd, 5 Mornington Road, Woodford Green, Essex IG8 0TU, (GB)
PATENT (CC, No, Kind, Date): EP 903887 A2 990324 (Basic)
EP 903887 A3 990616
EP 903887 B1 040609
APPLICATION (CC, No, Date): EP 98124151 920903;
PRIORITY (CC, No, Date): US 759314 910913
DESIGNATED STATES: DE; FR; GB; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 532227 (EP 92307999)
INTERNATIONAL PATENT CLASS: H04L-009/32; H04Q-007/38
ABSTRACT WORD COUNT: 185
NOTE:
Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199911	734
CLAIMS B	(English)	200424	963
CLAIMS B	(German)	200424	855
CLAIMS B	(French)	200424	1164
SPEC A	(English)	199911	6063
SPEC B	(English)	200424	6026
Total word count - document A			6798
Total word count - document B			9008
Total word count - documents A + B			15806

...SPECIFICATION before, perhaps a portion of the RAND signal), i.e., in plaintext. Once the authentication sequence is **verified** , the **base station** can process the call and make the connection to the called party.
The protocol for connecting to...

...SPECIFICATION before, perhaps a portion of the RAND signal), i.e., in plaintext. Once the authentication sequence is **verified** , the **base station** can process the call and make the connection to the called party.
The protocol for connecting to...

11/3,K/18 (Item 18 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00953220
AUTHENTICATION KEY MANAGEMENT FOR MOBILE STATIONS
AUTHENTIFIZIERUNGSSCHLUSSELVERWALTUNG FUR MOBILE STATIONEN
GESTION DE CLES D'AUTHENTIFICATION POUR STATIONS MOBILES
PATENT ASSIGNEE:
ERICSSON INC., (1203498), 7001 Development Drive, P.O. Box 13969, Research Triangle Park, NC 27709, (US), (Proprietor designated states: all)
INVENTOR:
FEHNEL, Michael, David, 3021 Bentwillow Drive, Fuquay-Varina, NC 27526, (US)
LEGAL REPRESENTATIVE:
O'Connell, David Christopher et al (62551), Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 6UD, (GB)
PATENT (CC, No, Kind, Date): EP 965240 A2 991222 (Basic)
EP 965240 B1 021218
WO 98019493 980507
APPLICATION (CC, No, Date): EP 97913877 971027; WO 97US19662 971027
PRIORITY (CC, No, Date): US 739259 961030
DESIGNATED STATES: BE; DE; FI; FR; GB; IT; SE
INTERNATIONAL PATENT CLASS: H04Q-007/38
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200251	684
CLAIMS B	(German)	200251	611
CLAIMS B	(French)	200251	768
SPEC B	(English)	200251	7321
Total word count - document A			0
Total word count - document B			9384
Total word count - documents A + B			9384

...SPECIFICATION the serving base station. Each mobile station also stores its SSD in memory.
In the process of **authentication** , the **base station** generates and sends to the mobile station a random bit pattern, called RAND or RANDU, on the...

11/3,K/44 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00545506
METHOD FOR AUTHENTICATING A SOURCE OF COMMUNICATION IN A COMMUNICATION SYSTEM

PROCEDE D'AUTHENTIFICATION D'UNE SOURCE DE COMMUNICATION DANS UN SYSTEME DE COMMUNICATION
Patent Applicant/Assignee:
MOTOROLA INC,
Inventor(s):
BROWN Daniel Peter,
OPRESCU-SURCOBE Valentin,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200008879 A1 20000217 (WO 0008879)
Application: WO 99US12454 19990604 (PCT/WO US9912454)
Priority Application: US 98130417 19980806
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
BR JP KR AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 3019
Fulltext Availability:
Detailed Description

Detailed Description
... are allowed to function in the communication system. However, in most instances, the mobile stations do not **authenticate** the **base stations** which are also sources of communication in the system.

The mobile stations are also vulnerable to unauthorized...

...whereby the network authenticates the user and the user authenticates the network.

A traditional means of performing **mutual authentication** requires the mobile station and the **base station** network to transmit challenge numbers to each other, to calculate responses, to transmit the responses, and to...

...step. In any case, the source of the second communication may be the mobile station or the **base station** . As such, the invention provides an efficient method of **mutual authentication** during any state of the mobile station.

At the receiving end of the second communication, the token...

11/3,K/47 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00489958 **Image available**
METHOD, ACCESS POINT DEVICE AND PERIPHERAL FOR PROVIDING SPACE DIVERSITY IN A TIME DIVISION DUPLEX WIRELESS SYSTEM
PROCEDE, DISPOSITIF DE POINT D'ACCES, ET PERIPHERIQUES ASSURANT LA DIVERSITE D'ESPACE DANS UN SYSTEME DUPLEX SANS FIL EN TEMPS PARTAGE
Patent Applicant/Assignee:
MOTOROLA INC,
Inventor(s):
EASTMOND Bruce Charles,
CUDAK Mark Conrad,
KEPLER James Frank,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9921310 A1 **19990429**
Application: WO 98US14868 19980717 (PCT/WO US9814868)
Priority Application: US 97954770 19971020
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

CN DE GB
Publication Language: English
Fulltext Word Count: 24480
Patent and Priority Information (Country, Number, Date):
Patent: ... **19990429**
Fulltext Availability:
Detailed Description
Publication Year: **1999**

Detailed Description
... message. The peripheral would compare the challenge response with one generated locally and if they match the **access point** has been **authenticated** .. Likewise, the access point may initiate authenticate the network using the same Authenticity Challenge and Challenge Response...

```
File 347:JAPIO Nov 1976-2004/Dec(Updated 050405)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200524
         (c) 2005  Thomson Derwent

Set     Items   Description
S1      64102   ACCESS()POINT? ? OR AP OR APS OR BASE()STATION? ? OR WIREL-
             ESS()(ROUTER? ? OR GATEWAY? ?)
S2         42   S1(5W)(AUTHENTICATED OR VALIDATED OR VERIFIED)
S3          0   S1(5W)((AUTHENTICATE OR AUTHENTICATES OR AUTHENTICATING OR
             VALIDATE OR VALIDATES OR VALIDATING)(1W)(ITSELF OR OWN()SELF -
             OR THEMSELVES))
S4         31   (AUTHENTICAT??? OR VALIDAT??? OR VERIF?)(1W)S1
S5        333   MUTUAL?()(AUTHENTICAT??? OR VALIDAT??? OR VERIF?)
S6          8   S1(10N)S5
S7         71   (S2 OR S4 OR S6)
S8         23   S7 AND AC=US/PR
S9          8   S8 AND AY=(1985:1999)/PR
S10        13   S7 AND PY=1985:1999
S11        16   S9:S10
S12        34   (BIDIRECTIONAL OR BI()DIRECTIONAL)()(AUTHENTICAT??? OR VAL-
             IDAT??? OR VERIF? OR CHECK???)
```

11/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06301020 **Image available**
SYSTEM FOR VERIFICATION AND COMPUTER READABLE STORAGE MEDIUM STORING PROGRAM FOR VERIFICATION

PUB. NO.: 11-242615 [JP 11242615 A]
PUBLISHED: September 07, 1999 (**19990907**)
INVENTOR(s): ARAI RITSUKO
KAYANO SHINICHIRO
SUZUKI KENJI
APPLICANT(s): MITSUBISHI ELECTRIC CORP
APPL. NO.: 10-044113 [JP 9844113]
FILED: February 25, 1998 (19980225)
INTL CLASS: G06F-011/28; G06F-011/26; G06F-013/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a system for verification with which verifying work can be performed while reproducing the same system as a system to be verified without being affected by the configuration of an information processor for verification to be used for the system for verification.
SOLUTION: Concerning this system, a means 7 for executing a program to be verified can be provided. In this case, this executing means 7 executes plural application(**AP**) programs 3 to be **verified** on an information processor 6 for verification having a virtual network memory 9 for storing data transmitted from the **AP** programs 3 to be **verified** while classifying them and stores the data transmitted from these **AP** programs 3 to be **verified** on the virtual network memory 9 according to the said classification.

11/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

06222812
METHOD FOR INITIALIZING CONNECTION BETWEEN MOBILE TERMINAL AND IN-HOME BASE STATION

PUB. NO.: 11-164374 [JP 11164374 A]
PUBLISHED: June 18, 1999 (**19990618**)
INVENTOR(s): BLANKE GERO
FRANCIS PINAULT
MESSIET SAMIRA
APPLICANT(s): ALCATEL CIT
APPL. NO.: 10-265922 [JP 98265922]
FILED: September 21, 1998 (19980921)
PRIORITY: 9711834 [FR 11834], FR (France), September 23, 1997 (19970923)
9803701 [FR 371], FR (France), March 25, 1998 (19980325)
INTL CLASS: H04Q-007/38; H04Q-007/34

ABSTRACT

PROBLEM TO BE SOLVED: To initialize connection between a mobile terminal of a public mobile communication network and an in-home base station by authenticating the mobile terminal, transmitting data which initializes connection to the in-home base station from the public mobile communication network to a terminal and transmitting the data to the in-home **base**

station .

SOLUTION: A mobile terminal is **authenticated** by a public mobile communication network, data that initializes connection with an in-home base station is transmitted from the public mobile communication network to a terminal and the data is transmitted from the mobile terminal to the in-home base station. That is, connection initialization data, especially, a frequency or a channel which is used to set connection, a start frequency, change rules of a frequency or an allowable maximum output and other parameters that are effective to connection in a more general sense are transmitted from the public mobile communication network to the mobile terminal. These data are transmitted, e.g., by an operator of the public mobile communication network, and the operator manages a frequency that is locally used with the mobile terminal.

11/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

06213458 **Image available**
TELEPHONE DEVICE PROVIDED WITH BASE STATION AND AT LEAST ONE HANDSET, HANDSET SUBSCRIBING METHOD AND HANDSET AND BASE STATION SUITABLE FOR TELEPHONE DEVICE

PUB. NO.: 11-155019 [JP 11155019 A]
PUBLISHED: June 08, 1999 (**19990608**)
INVENTOR(s): LORIEAU CHRISTOPHE
APPLICANT(s): KONINKL PHILIPS ELECTRON NV
APPL. NO.: 10-252733 [JP 98252733]
FILED: September 07, 1998 (19980907)
PRIORITY: 9711239 [FR 11239], FR (France), September 10, 1997 (19970910)
INTL CLASS: H04M-001/66; H04Q-007/38; H04L-009/32; H04M-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To prevent the fraudulent subscription of a handset by providing a ciphering means for ciphering subscriber data with respect to a telephone device having a subscribing means by which the handset and a **base station** are **validated** by means of subscriber data.
SOLUTION: The handset HS1 is provided with a communication assembly 40 having an antenna 41 so as to execute communication with the base station BS or with another handset HS2, etc., from it. When the handset subscribes the base station, three kinds of data stored in a read only memory 56, that is, identifier data of the base station where the handset subscribes, authenticating key data and data supplied to the subscribing base station by its own identifier are saved and stored in a ciphered shape in the read only memory 56. The data are extracted from the read only memory 56 and a prescribed box so as to be reversely converted before utilization for another box. Another handset is not used for subscriber data because of the existence of numbers which are assigned to the respective handsets.

11/5/5 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013846142 **Image available**
WPI Acc No: 2001-330355/200135
XRPX Acc No: N01-237865

Secure wireless LAN, has wireless device use by wireless device operator with access point connected to wired LAN in communication with wireless device through air channel authenticating wireless device

Patent Assignee: INTEL CORP (ITLC)
Inventor: GLENDINNING D; WEATHERSPOON S
Number of Countries: 025 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1081895	A1	20010307	EP 2000103334	A	20000221	200135	B

Priority Applications (No Type Date): US 99389437 A 19990903
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1081895	A1	E	13	H04L-012/28	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): EP 1081895 A1

NOVELTY - The network has a wireless device use by a wireless device operator. An access point connected to a wired LAN in communication with the wireless device through an air channel authenticating the wireless device. An authentication server connected to the wired LAN provides the operator with access to the wired LAN after **authenticating** the **access point** , the wireless device, and the operator.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for a method for operating a LAN

USE - For Secure wireless LAN.

ADVANTAGE - Inexpensive, easy to set up, fast, and reliable.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the network of the invention.

pp; 13 DwgNo 2/3

Title Terms: SECURE; WIRELESS; LAN; WIRELESS; DEVICE; WIRELESS; DEVICE; OPERATE; ACCESS; POINT; CONNECT; WIRE; LAN; COMMUNICATE; WIRELESS; DEVICE ; THROUGH; AIR; CHANNEL; AUTHENTICITY; WIRELESS; DEVICE
Derwent Class: W01
International Patent Class (Main): H04L-012/28
International Patent Class (Additional): H04L-029/06
File Segment: EPI

11/5/6 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

013023970
WPI Acc No: 2000-195821/200017
XRPX Acc No: N00-144861

Source authenticating method for cellular communication, involves using data token field generated during communication between mobile and base station, to produce burst of data for subsequent communication

Patent Assignee: MOTOROLA INC (MOTI)
Inventor: BROWN D P; OPRESCU-SURCOBE V
Number of Countries: 021 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200008879	A1	20000217	WO 99US12454	A	19990604	200017	B

Priority Applications (No Type Date): US 98130417 A 19980806
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200008879	A1	E	14	H04Q-007/20	

Designated States (National): BR JP KR
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Abstract (Basic): WO 200008879 A1

NOVELTY - Communication between mobile station and **base station**, is **authenticated** based on which a token field of data which authenticate the next communication between mobile and base station, is generated. Then, the token field of data is added to a data field, to produce a burst of data for the next communication between mobile and base station.

DETAILED DESCRIPTION - The communication occurs after mobile station or base station switches from inactive state to active state. The next communication occurs after the mobile station switches from a quasi active state to active state.

USE - For authenticating source of communication in cellular communication system.

ADVANTAGE - Authentication of subsequent communication between base and mobile stations is performed with minimal overhead in over-the-air communication, thus permits efficient method of authenticating source of communication.

pp; 14 DwgNo 0/0

Title Terms: SOURCE; AUTHENTICITY; METHOD; CELLULAR; COMMUNICATE; DATA; TOKEN; FIELD; GENERATE; COMMUNICATE; MOBILE; BASE; STATION; PRODUCE; BURST; DATA; SUBSEQUENT; COMMUNICATE

Derwent Class: W01; W02

International Patent Class (Main): H04Q-007/20

File Segment: EPI

11/5/7 (Item 4 from file: 350)

DIALOG(R)File 350:Derwent WPIX

012729780 **Image available**

WPI Acc No: 1999-535893/ **199945**

XRPX Acc No: N99-398596

User information transmission procedure for mobile communication system - involves receiving assignment information for control channel to transmit user information to base station

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11234738	A	19990827	JP 9837024	A	19980219	199945	B

Priority Applications (No Type Date): JP 9837024 A 19980219

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11234738	A		16	H04Q-007/36	

Abstract (Basic): JP 11234738 A

NOVELTY - When user information is to be transmitted from mobile terminal to base station, assignment information of control channel is received through empty control channel, after receiving **authentication** from **base station** via access channel. Then, user information is transmitted to base station via assigned control channel. DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following: apparatus used for performing user information transmission procedure; recording medium stored with user information transmission program

USE - For transmitting user information to base station in mobile communication system.

ADVANTAGE - Control channel is used effectively. Number of terminal accommodations of base station is increased.

Dwg.1/22

Title Terms: USER; INFORMATION; TRANSMISSION; PROCEDURE; MOBILE; COMMUNICATE; SYSTEM; RECEIVE; ASSIGN; INFORMATION; CONTROL; CHANNEL; TRANSMIT; USER; INFORMATION; BASE; STATION

Derwent Class: W01; W02

International Patent Class (Main): H04Q-007/36
International Patent Class (Additional): H04Q-007/28; H04Q-007/34
File Segment: EPI

11/5/9 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012376973 **Image available**
WPI Acc No: 1999-183080/ **199916**
Related WPI Acc No: 1993-087215
XRPX Acc No: N99-134493
Authentication method for mobile station in e.g. cellular telephone system
Patent Assignee: AT & T CORP (AMTT)
Inventor: REEDS J A; TREVENTI P A; YU I
Number of Countries: 004 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 903887	A2	19990324	EP 92307999	A	19920903	199916 B
			EP 98124151	A	19920903	
EP 903887	B1	20040609	EP 92307999	A	19920903	200438
			EP 98124151	A	19920903	
DE 69233365	E	20040715	DE 92633365	A	19920903	200446
			EP 98124151	A	19920903	

Priority Applications (No Type Date): US 91759314 A 19910913
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 903887	A2	E	17	H04L-009/32	Div ex application EP 92307999 Div ex patent EP 532227
	Designated States (Regional): DE FR GB SE				
EP 903887	B1	E		H04L-009/32	Div ex application EP 92307999 Div ex patent EP 532227
	Designated States (Regional): DE FR GB SE				
DE 69233365	E			H04L-009/32	Based on patent EP 903887

Abstract (Basic): EP 903887 A2
NOVELTY - Base station contacts service provider to obtain datum and then **authenticates** string. **Base station** can direct mobile unit to regenerate datum or create new one.
USE - For cellular telephone, fax or modem.
ADVANTAGE - Secure due to performing independent identification of caller at time when connection is established. Improved privacy.
DESCRIPTION OF DRAWING(S) - The drawing shows a group of network providers and cellular radio providers which are interconnected using mobile and stationary telephones.
pp; 17 DwgNo 1/11
Title Terms: AUTHENTICITY; METHOD; MOBILE; STATION; CELLULAR; TELEPHONE; SYSTEM
Derwent Class: W01; W02
International Patent Class (Main): H04L-009/32
International Patent Class (Additional): H04Q-007/38
File Segment: EPI

11/5/15 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008771943 **Image available**
WPI Acc No: 1991-275958/ **199138**
XRPX Acc No: N91-210804
Checking comprehensive authentication in mobile telephone system -

incorporating bidirectional checks between mobile and base stations to prevent false base stations establishing mobile subscription

Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF); ERICSSON OY AB L M (TELF)

Inventor: DAHLIN J E A; RAITH A K; WILKINSON D P; DAHLIN J E A S; DENT P W; DAHLIN J E; AKE J E; DENT W P; DENT W; RAITH A; DAHLIN J E S

Number of Countries: 029 Number of Patents: 028

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 447380	A	19910918	EP 91850016	A	19910120	199138 B
WO 9114348	A	19910919				199140
SE 9000856	A	19910910				199144
SE 465800	B	19911028				199146
AU 9174952	A	19911010				199201
FI 9105237	A	19911106				199207
NO 9104357	A	19911107				199209
BR 9104907	A	19920414	BR 914907	A	19910129	199222
			WO 91SE66	A	19910129	
CN 1054868	A	19910925	CN 91101527	A	19910309	199226
JP 4505693	W	19921001	JP 91505884	A	19910129	199246
			WO 91SE66	A	19910129	
PT 96979	A	19930430	PT 96979	A	19910308	199321
TW 199250	A	19930201	TW 91100981	A	19910207	199327
NZ 236936	A	19930727	NZ 236936	A	19910129	199333
AU 638820	B	19930708	AU 9174952	A	19910129	199334
US 5282250	A	19940125	US 91655771	A	19910215	199405
			US 9368234	A	19930527	
US 5390245	A	19950214	US 91655771	A	19910215	199512
			US 9343758	A	19930407	
			US 9368234	A	19930527	
EP 447380	B1	19950412	EP 91850016	A	19910129	199519
DE 69108762	E	19950518	DE 608762	A	19910129	199525
			EP 91850016	A	19910129	
CN 1024241	C	19940413	CN 91101527	A	19910309	199527
ES 2073726	T3	19950816	EP 91850016	A	19910129	199539
SG 9590931	A	19951222	SG 9590931	A	19950526	199611
IE 67887	B	19960501	IE 91544	A	19910218	199629
US 5559886	A	19960924	US 91655771	A	19910215	199644
			US 9343758	A	19930407	
			US 9368234	A	19930527	
			US 94298782	A	19940831	
NO 300249	B1	19970428	WO 91SE66	A	19910129	199724
			NO 914357	A	19911107	
FI 102134	B1	19981015	WO 91SE66	A	19910129	199847
			FI 915237	A	19911106	
PH 30204	A	19970205	PH 42018	A	19910218	199953
KR 144560	B1	19980817	KR 91701553	A	19911108	200022
CA 2051385	C	20010403	CA 2051385	A	19910129	200124
			WO 91SE66	A	19910129	

Priority Applications (No Type Date): SE 90856 A 19900309

Cited Patents: DE 3405381; DE 3420460; US 4436957

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 447380	A		7		
Designated States (Regional): AT BE CH DE ES FR GB GR IT LI LU NL					
WO 9114348	A				
Designated States (National): AU BR CA FI JP KR NO					
BR 9104907	A			H04Q-007/02	Based on patent WO 9114348
CN 1054868	A			H04B-007/26	
JP 4505693	W		5	H04B-007/26	Based on patent WO 9114348
PT 96979	A			H04Q-007/02	
TW 199250	A			H04B-007/26	
NZ 236936	A			H04B-007/26	
AU 638820	B			H04Q-007/02	Previous Publ. patent AU 9174952

				Based on patent WO 9114348
US 5282250	A	7	H04L-009/32	Cont of application US 91655771
US 5390245	A	5	H04L-009/32	Cont of application US 91655771 Cont of application US 9368234 Cont of patent US 5282250
EP 447380	B1 E	8	H04Q-007/22	
Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LI LU NL				
DE 69108762	E		H04Q-007/22	Based on patent EP 447380
CN 1024241	C		H04B-007/26	
ES 2073726	T3		H04Q-007/22	Based on patent EP 447380
SG 9590931	A			Previous Publ. patent EP 447380
IE 67887	B		H04Q-007/04	
US 5559886	A	6	H04L-009/00	Cont of application US 91655771 Cont of application US 9343758 Cont of application US 9368234 Cont of patent US 5220605 Cont of patent US 5282250 Cont of patent US 5390245
NO 300249	B1		H04B-007/26	Previous Publ. patent NO 9104357
FI 102134	B1		H04Q-007/38	Previous Publ. patent FI 9105237
PH 30204	A		H04L-009/32	
KR 144560	B1		H04Q-007/02	
CA 2051385	C E		H04Q-007/02	Based on patent WO 9114348

Abstract (Basic): EP 447380 A

The method involves establishing a connection in which the base station sends a question concerning the authentication of the mobile station and orders the mobile to send a first response signal (Resp 1) which is used in the base station to establish the authentication.

Subsequent to establishing the authentication of the mobile (2,3,4) in the base station, there is sent from the base station a second response signal (Resp 2) to the mobile, which forms (8) a corresp. second response signal (Resp 2) in order to establish (9) the authentication of the base station. When this authentication is established, the mobile sends a third response signal (Resp 3) and establishes the authentication of the mobile prior to the connection being established.

USE - E.g. for paging systems. (7pp Dwg.No.2/2)

Title Terms: CHECK; COMPREHENSIVE; AUTHENTICITY; MOBILE; TELEPHONE; SYSTEM; INCORPORATE; BIDIRECTIONAL; CHECK; MOBILE; BASE; STATION; PREVENT; FALSE; BASE; STATION; ESTABLISH; MOBILE; SUBSCRIBER

Derwent Class: W01; W02; W05

International Patent Class (Main): H04B-007/26; H04L-009/00; H04L-009/32; H04Q-007/02; H04Q-007/04; H04Q-007/22; H04Q-007/38

International Patent Class (Additional): H04M-001/66; H04M-001/72; H04Q-001/66; H04Q-007/06

File Segment: EPI